

## A SECURE METHOD OF EXCHANGING INFORMATION MESSAGES

### BACKGROUND OF THE INVENTION

#### Field of the invention

The invention relates to a secure method of  
5 exchanging information messages sent successively, at  
given time intervals, from a sending platform to a  
receiving platform. The invention relates more  
particularly to a method which ensures that the last  
message picked up by the receiving platform corresponds  
10 to the last message sent by the sending platform.

#### Description of the prior art

The method according to the invention finds one  
application in train control and/or supervision systems,  
which are known in France as control, operation and  
15 maintenance aid systems (SACEM) and include a centralized  
control station, fixed installations along the tracks,  
and a control unit in each train. In control systems of  
this kind, the centralized control station sends the  
fixed installations at regular time intervals information  
20 messages including information relating to traffic  
conditions on one or more track sections downstream of  
the fixed installation. The control unit of any train in  
the network then receives from the fixed installations  
the last information message received by the fixed  
25 installation and deduces therefrom the running speed to  
adopt. When exchanging information messages of the above  
kind it is essential, for safety reasons, to be sure that  
the last message received by the fixed installations  
corresponds to the last information message sent by the  
30 centralized control station. Given the various components  
involved in transmitting messages, and the fact that  
there may be relatively great distances between the  
centralized control station and the fixed installations,  
it is possible for some messages to suffer interference  
35 or to be delayed during transmission and to reach the

fixed installations late, so modifying the order in which the fixed installation receives the information messages compared to the order in which they are sent by the centralized control station. In this case the updated  
5 information message at the fixed installation no longer corresponds to the last message sent by the centralized control station. Although such phenomena are rare, to ensure traffic safety it is absolutely essential that they are detected.

10 A standard way to make the transmission of information messages secure is to employ continuous bidirectional exchanges of data so that an information message received by a fixed installation is sent back to the centralized control station, which checks that it  
15 corresponds to the information message sent. However, methods of this kind relying on bidirectional exchanges of data use complex processing methods necessitating costly systems at the sender and the receiver.

The object of the present invention is therefore to  
20 propose a secure method of exchanging information messages which, in the course of successive unidirectional exchanges of information messages between a sending platform and a receiving platform, ensures that the last message picked up by the receiving platform  
25 corresponds to the last message sent by the sending platform, in order to be able to validate correct updating of the information message at the receiving platform.

#### SUMMARY OF THE INVENTION

30 To this end, the invention provides a secure method of exchanging information messages sent successively from a sending platform to a receiving platform which includes:

a) an initialization sequence in which an  
35 initialization message containing information relating to

a date  $t_1$  for sending a first information message  $M_1$  is exchanged between the sending platform and the receiving platform so that the sending platform and the receiving platform then both know the date  $t_1$  for sending the first  
5 information message  $M_1$ , and

b) an information message transmission sequence in which:

- the information messages are sent successively by the sending platform at given time intervals  $\Delta T_E$  with a  
10 sending time tolerance  $\delta$  ( $\delta < \Delta T_E$ ) based on a clock specific to the sending platform, so that the first message  $M_1$  is sent at the date  $t_1$  on the clock and the  $n$ th message  $M_n$  is sent at the date  $t_n = t_1 + (n-1) \cdot \Delta T_E + \delta$ , each message  $M_n$  being coded by means of a dynamic code  $C_n$   
15 specific to the date  $t_n$  of sending the message (the information message data is advantageously coded using a code defined as a function of the security criteria of the application, so that the information messages are rendered incomprehensible in the event of a transmission  
20 error, for example the SACEM code), and

- the messages received by the receiving platform are processed as a function of their reception date  $t_r$  based on a clock specific to the receiving platform so that the messages received in an observation  
25 window  $F_n$  in the vicinity of  $t_n$  are decoded using a decoding sequence  $DC_n$  adapted to decode the dynamic code  $C_n$ , the clock of the receiving platform being synchronized to the date  $t_1$  on receiving the first message  $M_1$ .

Particular embodiments of the method according to  
30 the invention can include one or more of the following features, individually or in any technically feasible combination:

- during the initialization sequence a) a coded initialization message  $M_0$  is sent from the sending  
35 platform to the receiving platform and a coded

initialization message  $M'_0$  is sent from the receiving platform to the sending platform, the initialization messages  $M_0$ ,  $M'_0$  containing the information relating to the date  $t_1$  for sending the first information message  $M_1$ ,  
5 and the initialization messages  $M_0$ ,  $M'_0$  being decoded by the sending platform and the receiving platform which then know the date  $t_1$  for sending the first information message  $M_1$ ;

- if the first message  $M_1$  is not received within an  
10 allotted time after reception of the initialization message, the clock of the sending platform is automatically synchronized to the date  $t_1$  at the moment corresponding to the end of the allotted time;
- the observation window  $F_n$  corresponds to a time  
15 window  $[t_1 + (n-1) \cdot \Delta T_E - \Delta T_F \cdot \varepsilon, t_1 + (n-1) \cdot \Delta T_E + \Delta T_F \cdot (1-\varepsilon)]$ , where  $n$  is an integer,  $\Delta T_F$  corresponds to the width of the observation window and satisfies the equation  $\Delta T_F \leq \Delta T_E$  and  $\varepsilon$  is from 0 to 1;
- a clock synchronization signal is sent regularly  
20 by the sending platform between sending messages  $M_n$ , the synchronization signal being used to correct the frequency or the phase of the internal clock of the receiving platform dynamically in order to reduce the phase or frequency error between the internal clocks of  
25 the receiving platform and the sending platform;
- the information messages decoded by the receiving platform are transmitted to an information processing module;
- the messages received by the receiving platform  
30 during an observation window  $F_n$  are stored sequentially in a memory able to store only one message at a time and only the message stored in the memory at the end of the observation window  $F_n$  is transmitted to the information processing module; and
- the sending platform is part of a centralized  
35

control station of a rail traffic supervision and control system, the receiving platform is part of a fixed installation disposed alongside a rail track, and the information processing module is a control unit on board  
5 a train circulating on a track section associated with the fixed installation.

Objects, aspects and advantages of the present invention will be better understood from the following description of one particular embodiment of the  
10 invention, which is offered by way of non-limiting example and refers to the accompanying drawings.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 is a partial diagrammatic representation of a train supervision installation employing a secure  
15 method in accordance with the invention of exchanging information messages.

Figure 2 is a flowchart showing the main steps of a sending method conforming to the secure exchange method according to the invention employed by a sending  
20 platform.

Figure 3 is a flowchart showing the main steps of a processing method conforming to the secure exchange method according to the invention employed by a receiving platform.

25 Figure 4 is a timing diagram showing the sending of information messages from the sending platform, the reception of the messages at the receiving platform, and the processing of the messages in conformance with the secure exchange method according to the invention.

30 To clarify the drawings, only the system components necessary for understanding the invention are shown. The same components carry the same reference numbers if shown in more than one figure.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

35 Figure 1 shows diagrammatically a centralized

control station 1 communicating to fixed installations 2 disposed alongside a rail track section information messages including information relating to traffic conditions on one or more track sections downstream of the fixed installation 2. The messages are then transmitted, in a manner that is known in the art, from the fixed installations 2 via a track circuit to a train 5 which carries a control unit 6 which uses the information messages to determine, among other things, how to proceed, for example the speed to adopt or if it is necessary to initiate an emergency stop.

For transmitting the information messages, the centralized control station 1 includes a sending platform 10 connected by transmission cables 4 to a receiving platform 20 in the fixed installation 2. The sending platform 10 and the receiving platform 20 each have an internal clock.

The sequence of information messages sent by the sending platform 10 using the secure exchange method according to the invention is described next with reference to figure 2.

In that figure, in a first step 101 of the secure exchange method, an initialization sequence is executed during which a coded initialization message  $M_0$  is transmitted from the sending platform 10 to the receiving platform 20. The message  $M_0$  contains a portion of the information of the initial date of the first information message, for example a random number, generated by the sending platform. In a second step 102, the sending platform receives the message  $M'_0$  sent by the receiving platform. The message  $M'_0$  contains a portion of the information of the initial date of the first information message, for example a random number, generated by the receiving platform. In a step 103 the sending platform 10 decodes the messages  $M_0$ ,  $M'_0$  to generate the initial date

of the first message. An implicit portion can optionally complement the initial date.

The transmission of the initialization sequence is conventionally made secure by executing a bidirectional  
5 exchange method to check that the correlation between the received message and the sent message is correct.

The initialization sequence previously described is followed by a step 104 of the method in which no message is sent by the sending platform 10 until the time  $t_e$  on  
10 the internal clock of the sending platform 10 reaches the date  $t_1$  for sending the first message  $M_1$ . At that date  $t_1$ , the sending platform 10 sends the first message  $M_1$ , after which messages are sent at constant time intervals  $\Delta T_e$  such that the  $n$ th message  $M_n$  is sent at the date  
15  $t_n = t_1 + (n-1) \cdot \Delta T_e + \delta$ , where  $n$  is an integer and  $\delta$  is the sending time tolerance ( $\delta < \Delta T_e$ ).

According to one feature of the invention, each message  $M_n$  sent is coded with a dynamic code  $C_n$  specific to the date  $t_n$  for sending the message. The dynamic code  $C_n$   
20 is of a type chosen from dynamic codes known in the art which have coding properties such that the decoding of the message  $M_n$  using a decoding sequence other than the decoding sequence  $DC_n$  for decoding the code  $C_n$  produces a message that is incomprehensible given the coding defined  
25 at the level of the application. For example, the code chosen can be a superimposed pseudo-random sequence based on applying to each of the data bits the primitive polynomial  $X^{32} + X^{22} + X^2 + X + 1$ .

The processing executed in parallel by the  
30 receiving platform 20 while the sending platform 10 is sending the sequence of information messages is described next with reference to figure 3.

As shown in figure 3, in a first step 201 of the method, the receiving platform 20 receives the message  $M_0$   
35 contained in the initialization sequence sent by the

sending platform during the step 101. In a second step 202, the receiving platform 20 sends the message  $M'_0$ , which is received by the sending platform during the step 102. In a step 203, the messages  $M_0$ ,  $M'_0$  are decoded by the  
5 receiving platform 20 to obtain the initial date  $t_1$  of the first message  $M_1$ , as in step 103 of the method as executed at the sending platform.

In a subsequent step 204 of the method, which is triggered when the receiving platform 20 receives the  
10 first message  $M_1$ , the internal clock of the receiving platform 20 is synchronized to the date  $t_1$  so that  $t_r = t_1$  at the time the first message  $M_1$  is received, where  $t_r$  is the time on the internal clock of the receiving platform 20. The internal clock of the receiving platform 20 is  
15 synchronized by default to the date  $t_1$  if the first message  $M_1$  does not reach the receiving platform 20 within an allotted time after reception of the initialization message  $M_0$ .

After the message  $M_1$  is received, the clock of the  
20 receiving platform 20 is preferably synchronized regularly to the clock of the sending platform 10 using clock synchronization frames sent regularly by the sending platform 10 in the same cycle as the messages  $M_n$ . These frames are either dedicated frames or the messages  
25  $M_n$  themselves. Accordingly, if a synchronization error (phase, frequency, average, least squares, etc.) is measured between the internal clock of the sending platform 10 and the internal clock of the receiving platform 20, the frequency or the phase of the internal  
30 clock of the receiving platform 20 is corrected dynamically to reduce the phase or frequency error between the two clocks.

During the next step 205 of the method, the first message  $M_1$  received is decoded by means of a decoding  
35 sequence  $DC_1$  adapted to decode the dynamic code  $C_1$  and the

result of decoding the message  $M_1$  is transmitted to the track circuit by the receiving platform 20.

The next step 206 of the method is triggered iteratively when the receiving platform 20 receives a new message  $M_r$ , a priori the message  $M_n$ , at a time  $t_r$  in an observation time window  $F_n$  that corresponds to a time window  $[t_1 + (n-1) \cdot \Delta T_e - \Delta T_f \cdot \varepsilon, t_1 + (n-1) \cdot \Delta T_e + \Delta T_f \cdot (1-\varepsilon)]$ , where  $\Delta T_f$  is the width of the observation window,  $n$  is an integer and  $\varepsilon$  is from 0 to 1.

During the next step 207 of the method, the message  $M_r$  received from the sending platform 20 in an observation window  $F_n$  is decoded using a decoding sequence  $DC_n$  allotted to the observation window  $F_n$  which corresponds to the inverse coding sequence  $DC_n$  and is adapted to decode only the dynamic code  $C_n$  of the  $n$ th message sent by the sending platform 10.

In a preferred embodiment of the invention, in a step that is not shown in figure 3, the message  $M_r$  decoded by the receiving platform 20 is then stored temporarily in a memory having a capacity such that it is able to store only one message at a time, before being sent to the track circuit at the time  $t_r$  corresponding to the end of the observation window  $F_n$ . In a simplified variant, the message  $M_r$  can be transmitted to the track circuit immediately at the end of the step 207, without being stored in a memory.

The train 5 on the track section then receives, via the track circuit, the messages decoded by the receiving platform 20, with the assurance that the messages  $M_r$  received, which are comprehensible given the decoding defined in the application, are correctly updated messages  $M_n$ , the information in which must be acted on. Moreover, to ensure the safety of trains circulating on the track, the control unit 6 on board the train 5 triggers an emergency stop if the train 5 receives a

plurality of successive incomprehensible messages, for example five such messages one after the other, with a result that the train is stopped when it no longer has sufficient information on traffic conditions in the downstream track section.

Figure 4 shows one example of a sequence of information messages exchanging in conformance with a method according to the invention. In this figure, the sending of messages  $M_1$  to  $M_6$  is shown on the top axis  $t_e$ , this axis corresponding to the time on the internal clock of the sending platform 10, and the reception of messages is shown on the axis  $t_r$  corresponding to the time on the clock of the receiving platform 20. In the example described with reference to Figure 4, the initialization sequence, not shown in this figure, is considered to be initiated at the time  $t_e = 4h59min$  and the date  $t_1$  of sending the first message is considered to be  $t_1 = 5h$ . The interval  $\Delta T_e$  is of the order of a few milliseconds, for example  $\Delta T_e = 50$  ms, with the result that the updating of the information messages is regular. In the example shown, the sending time tolerance  $\delta$  is zero and the observation windows  $F_n$  have the characteristics  $\varepsilon = 0.5$  and  $\Delta T_r = 25$  ms.

Accordingly, referring to figure 4, and in particular to the reception of messages shown on the bottom axis  $t_r$  representing the time on the clock of the receiving platform 20, a few moments after the first message  $M_1$  is sent the receiving platform 20 receives the message  $M_1$ . The receiving platform 20 then synchronizes its internal clock so that  $t_r = t_1$  at the moment the message  $M_1$  is received. The message  $M_1$  is then decoded by the receiving platform using the decoding sequence  $DC_1$  and is then transmitted to the track circuit and thus to any train 5 on the track section.

A few moments later, the receiving platform 20

receives the message  $M_2$  in an observation window  $F_2$  of width  $\Delta T_F$  centered on  $t_2$ . The receiving platform 20 then decodes the message  $M_2$  using the decoding sequence  $DC_2$ . The decoded message is stored in a memory of the receiving platform having a capacity able to store only one message at a time and is then transmitted to the track circuit at the time  $t_r$  corresponding to the end of the observation window  $F_2$ :  $t_r = t_2 + \Delta T_F / 2$ . The control unit 6 of the train 5 on the track section is then informed of traffic conditions by the message  $M_2$ .

Because of interference affecting the transmission of the message  $M_3$ , the receiving platform 20 does not receive any message during the observation window  $F_3$ . In this case, the message transmitted by the receiving platform 20 to the track circuit at the time  $t_r$  corresponding to the end of the observation window  $F_3$  is incomprehensible when decoded by the application, which informs the control unit 6 of the train 5 on the track section of this information message updating error.

In due course the message  $M_3$  is received in the observation window  $F_4$  and is then decoded using the decoding sequence  $DC_4$  allotted to the window  $F_4$ , which produces a decoded message that is incomprehensible, given the coding defined by the application and stored in the memory of the receiving platform 20. The incomprehensible message is transmitted to the track circuit at a time  $t_r$  corresponding to the end of the observation window  $F_4$  and the control unit 6 of the train 5 receives the incomprehensible message and interprets it as another information message updating error. The control unit 6 then registers two successive information message updating errors, but does not yet bring about emergency stopping of the train if the allowed tolerance is five successive errors.

Two messages  $M_4$  and  $M_5$  are received successively by

the receiving platform 20 during an observation window  $F_5$ . The receiving platform 20 receives the message  $M_4$  first and then the message  $M_5$  in the same observation window  $F_5$ . The receiving platform decodes the message  $M_5$  using the  
5 decoding sequence  $DC_5$ , producing a decoded message that is comprehensible, given the coding defined by the application and stored in the memory of the receiving platform 20 in place of the preceding message. The message  $M_5$  is transmitted to the track circuit at a time  
10  $t_r$  corresponding to the end of the observation window  $F_5$ . The control unit 6 of the train 5 then receives a message which is comprehensible, given the coding defined by the application, i.e. the message  $M_5$ , with the assurance that the information contained in that message has been  
15 updated correctly.

During an observation window  $F_6$ , the receiving platform 20 receives the message  $M_6$ , which is decoded using the decoding sequence  $DC_6$  and then stored in the memory before it is sent to the track circuit at a time  $t_r$ ,  
20 corresponding to the end of the window  $F_6$ . The control unit 6 of the train 5 then receives a message that is comprehensible, given the coding defined by the application, i.e. the message  $M_6$ , with the assurance that the information contained in the message has been  
25 updated.

Thus, thanks to the regular unidirectional exchange of messages between a sending platform and a receiving platform, a secure method of exchanging information messages of the kind described above guarantees correct  
30 updating of the information messages that reach the destination in a comprehensible form, without using complex processing. A method of the above kind has the advantage that it is relatively inexpensive to implement and transmits information at high speed, unlike the usual  
35 bidirectional transmission systems, in which the

information verification sequence considerably slows the transmission of messages, and therefore action taken in response to them. The method according to the invention therefore refreshes information messages received by a  
5 train at a relatively high rate.

Of course, the invention is in no way limited to the embodiment described and shown, which is offered by way of example only and can be modified, in particular from the point of view of the composition of the various  
10 components or by substituting technical equivalents, without departing from the scope of protection of the invention.